UNITED STATES PATENT APPLICATION

of

Leon C. Wong,

Sudhanshu M. Aggarwal, and

Peter L. Beebee

for

METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO PRESENCE INFORMATION ACCORDING TO A VARIETY OF DIFFERENT ACCESS PERMISSION TYPES

BACKGROUND OF THE INVENTION

1. Cross-Reference to Related Applications

The present application claims the benefit of United States provisional application serial number 60/186,255, filed 29 February 2000, which provisional application is incorporated herein by reference.

2. The Field of the Invention

The present invention relates to the field of electronic communication. In particular, the present invention relates to methods and systems for controlling access to presence information according to a variety of different access permission types.

3. The Prior State of the Art

"Presence information" describes an availability status of a computer system or a user associated with that computer system. Presence information is useful in, for example, instant messaging in which electronic messages are rapidly communicated in a matter of seconds and often within a second. The rapid communication of instant messages facilitates real time electronic conversations among instant messaging participants. Therefore, instant messaging betters reflects the way people typically communicate over the phone or in person as compared to standard electronic mail.

One requirement for a real time conversation using instant messaging in that the participants be available for conversing. Presence information gives a participant a good idea on whether or not it would be beneficial to initiate or continue a conversation with another participant. For example, if the presence information for a given participant is "logged off", one might not bother composing an instant message for transmission to that

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

participant since the participant is not able to receive the instant message due to a disconnection from its instant messaging server. On the other hand, if the presence information for a given participant is "logged in", one might venture to compose and transmit an instant message since the participant will likely receive the instant message in real time. Whether or not there is a response to the instant message depends on whether or not the receiving participant is present at his/her computer and whether or not that participant chooses to respond. However, the presence information at least gives the sender the knowledge that the instant message will likely be received by the receiving participant's computer system in real time.

The presence information may give much more information regarding availability than whether the user's computer system is logged in or logged out. For example, the presence information might include "idle" indicating that even though the user is logged in, the user has not used the computer system for a while. Thus, a sender might conclude that even though the receiving computer system would receive the instant message in real time, that the user of the receiving computer system is not currently present at the computer system. Thus, the sender may elect not to compose and send an instant message since a real time reply is not likely. Other types of presence information might include, for example, "out to lunch" or "out, will be back at 3:00pm" and so forth.

Instant messaging is but one application in which presence information may be useful. Presence information might also be useful in office tracking software which tracks whether or not employees are available. If an employee is seen as not available, someone trying to contact the person might not bother to travel to the office of that employee or place a phone call to the employee.

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

It may often be desirable to control access to presence information. For example, a participant might not want someone else to know whether or not the individual is logged in or out to lunch. Thus, one might want to prohibit other individuals from viewing such presence information. Conventional systems for controlling access to presence information are limited in the sense that they only allow a user to control access in one particular way. Specifically, a user may simply be granted or denied the right to view presence information. Therefore, what are desired are methods and systems for controlling access to presence information according to a variety of different access permission types.

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

SUMMARY OF THE INVENTION

The present invention relates to methods and systems for controlling access to presence information using a number of different access permission types. Presence information is maintained over a computer network and describes availability of computers and associated users over that computer. For example, presence information may describe the availability of a computer using terms such as "logged in", "logged out", "active", "idle" and the like. The presence information may also describe the availability of a user associated with that computer using terms such as "out to lunch", "out of the office", "back at 3:00 pm" and the like. This presence information is useful in any application where the availability of a computer or a user associated with that computer is helpful. For example, in instant messaging, communication back and forth between users occurs quickly. If a user were not available to communicate in this fashion, there would often be no sense in sending an instant message to that user. Thus, instant messaging applications often involve maintaining presence information.

It may be desirable for a user to control who has access to presence information. For example, a user whose computer is "logged in" may not want others to know that the user is "logged in". Conventional ways of controlling access to presence information involve simply granting or denying the right to view presence information. However, the principles of the present invention allow for much finer control over the access to presence information. Specifically, the users are allowed to control access to presence information using a number of different access permission types. These types might include a permission to view presence information whether accurate or not, permission to view accurate presence information, permission to act on accessed presence information and so

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

forth. The permission to act on accessed presence information might include permission to send messages to the user associated with the accessed presence information and the like.

By using several different access permission types, the present invention enables finer control over access to presence information. For example, a user may grant the right to access presence information whether accurate or not, but deny the right to access accurate presence information. Thus, a user may indicate that the associated computer is "logged out" when, in fact, that is actually not the case. Other users may not ever even know that they are viewing inaccurate presence information. An embodiment of a method in accordance with the present invention works as follows.

An "owner" client computer system creates a request including an instruction to change an access permission status applicable to some or all of the other client computer systems network connected to the owner client computer system. This access permission status may be a right to view accurate presence information, a right to view any presence information, a right to act on the presence information and the like. The owner client computer system then transmits this request to a server computer system that maintains the presence information for the client computer systems.

Once, the server computer system receives this request, the server computer system sets an entry in a data field that represents the changed access permission status. Subsequently, when other client computer systems request a certain kind of access to the presence information, the server computer system will use the entry to determine whether or not that access should be granted.

Additional features and advantages of the invention will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by the practice of the invention. The features and advantages of the invention may

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. These and other features of the present invention will become more fully apparent from the following description and appended claims, or may be learned by the practice of the invention as set forth hereinafter.

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

BRIEF DESCRIPTION OF THE DRAWINGS

In order that the manner in which the above-recited and other advantages and features of the invention are obtained, a more particular description of the invention briefly described above will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only typical embodiments of the invention and are not therefore to be considered to be limiting of its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

Figure 1 illustrates an exemplary system that provides a suitable operating environment for the present invention;

Figure 2 is illustrates in more detail a networked computer that may be used in the operating environment of Figure 1;

Figure 3 illustrates a data structure that illustrates the type of presence information that the server system of Figure 1 may maintain;

Figure 4 illustrates a flowchart of a method of controlling access to the presence information;

Figure 5 illustrates in detail an extended data structure including access permissions for the owner client computer system; and

Figure 6 illustrates in detail a data structure of a request that includes an instruction to control access to presence information.

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

DETAILED DESCRIPTION OF THE INVENTION

The present invention extends to both methods and systems for controlling access to presence information. The embodiments of the present invention may comprise a special purpose or general purpose computer including various computer hardware, as discussed in greater detail below.

Embodiments within the scope of the present invention also include computer-readable media for carrying or having computer-executable instructions or data structures stored thereon. Such computer-readable media can be any available media which can be accessed by a general purpose or special purpose computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to carry or store desired program code means in the form of computer-executable instructions or data structures and which can be accessed by a general purpose or special purpose computer. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or a combination of hardwired or wireless) to a computer, the computer properly views the connection as a computer-readable medium. Thus, any such a connection is properly termed a computer-readable medium. Combinations of the above should also be included within the scope of computer-readable media. Computer-executable instructions comprise, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions.

Figure 1 and the following discussion are intended to provide a brief, general description of a suitable computing environment in which the invention may be

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

implemented. Although not required, the invention will be described in the general context of computer-executable instructions, such as program modules, being executed by computers in network environments. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Computer-executable instructions, associated data structures, and program modules represent examples of the program code means for executing steps of the methods disclosed herein. The particular sequence of such executable instructions or associated data structures represent examples of corresponding acts for implementing the functions described in such steps.

Those skilled in the art will appreciate that the invention may be practiced in network computing environments with many types of computer system configurations, including personal computers, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments where tasks are performed by local and remote processing devices that are linked (either by hardwired links, wireless links, or by a combination of hardwired or wireless links) through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

With reference to Figure 1, an exemplary system for implementing the invention includes a general purpose computing device in the form of a conventional computer 120, including a processing unit 121, a system memory 122, and a system bus 123 that couples various system components including the system memory 122 to the processing unit 121. The system bus 123 may be any of several types of bus structures including a memory bus

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. The system memory includes read only memory (ROM) 124 and random access memory (RAM) 125. A basic input/output system (BIOS) 126, containing the basic routines that help transfer information between elements within the computer 120, such as during start-up, may be stored in ROM 124.

The computer 120 may also include a magnetic hard disk drive 127 for reading from and writing to a magnetic hard disk 139, a magnetic disk drive 128 for reading from or writing to a removable magnetic disk 129, and an optical disk drive 130 for reading from or writing to removable optical disk 131 such as a CD-ROM or other optical media. The magnetic hard disk drive 127, magnetic disk drive 128, and optical disk drive 130 are connected to the system bus 123 by a hard disk drive interface 132, a magnetic disk drive-interface 133, and an optical drive interface 134, respectively. The drives and their associated computer-readable media provide nonvolatile storage of computer-executable instructions, data structures, program modules and other data for the computer 120. Although the exemplary environment described herein employs a magnetic hard disk 139, a removable magnetic disk 129 and a removable optical disk 131, other types of computer readable media for storing data can be used, including magnetic cassettes, flash memory cards, digital video disks, Bernoulli cartridges, RAMs, ROMs, and the like.

Program code means comprising one or more program modules may be stored on the hard disk 139, magnetic disk 129, optical disk 131, ROM 124 or RAM 125, including an operating system 135, one or more application programs 136, other program modules 137, and program data 138. A user may enter commands and information into the computer 120 through keyboard 140, pointing device 142, or other input devices (not shown), such as a microphone, joy stick, game pad, satellite dish, scanner, or the like.

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

These and other input devices are often connected to the processing unit 121 through a serial port interface 146 coupled to system bus 123. Alternatively, the input devices may be connected by other interfaces, such as a parallel port, a game port or a universal serial bus (USB). A monitor 147 or another display device is also connected to system bus 123 via an interface, such as video adapter 148. In addition to the monitor, personal computers typically include other peripheral output devices (not shown), such as speakers and printers.

The computer 120 may operate in a networked environment using logical connections to one or more remote computers, such as remote computers 149a and 149b. Remote computers 149a and 149b may each be another personal computer, a server, a router, a network PC, a peer device or other common network node, and typically include many or all of the elements described above relative to the computer 120, although only memory storage devices 150a and 150b and their associated application programs 136a and 136b have been illustrated in Figure 1. The logical connections depicted in Figure 1 include a local area network (LAN) 151 and a wide area network (WAN) 152 that are presented here by way of example and not limitation. Such networking environments are commonplace in office-wide or enterprise-wide computer networks, intranets and the Internet.

When used in a LAN networking environment, the computer 120 is connected to the local network 151 through a network interface or adapter 153. When used in a WAN networking environment, the computer 120 may include a modem 154, a wireless link, or other means for establishing communications over the wide area network 152, such as the Internet. The modem 154, which may be internal or external, is connected to the system bus 123 via the serial port interface 146. In a networked environment, program modules

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

depicted relative to the computer 120, or portions thereof, may be stored in the remote memory storage device. It will be appreciated that the network connections shown are exemplary and other means of establishing communications over wide area network 152 may be used.

Figure 2 illustrates a suitable network in which the present invention may operate and will be referred to frequently in describing embodiments of the present invention. The network includes a server computer system 210 that is network connectable to a plurality of client computer systems 220 including nine client computer systems 220a through 220i. Each of the server computer systems 210 and the client computer systems 220a through 220i may be structured as described above for the computer 120 of Figure 1 and include some or all of the components described as being included in the computer 120. However, many other computer devices may be used as the server computer system and client computer systems so long as they are consistent with the principles of the present invention as described herein.

In order to facilitate a clear understanding of the principles of the present invention, certain terms are hereinafter defined which are to be applied throughout this description and in the following claims.

In this description and in the following claims, a "client computer system" is defined as a computer or group of computers that use the services of another computer system. A "server computer system" is defined as a computer or group of computers that provides services to another computer system. A "computer" is defined as any device capable of processing data such as a personal computer, a personal digital assistant, and the like.

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

Note that a computer system may use the services of another computer system and yet still provide services to yet other computer systems. Thus, a client computer system in one context may also be a server computer system in another context. Similarly, a server computer system in one context may also be a client computer system in another context. The use of the term "server computer system" for computer system 210 and "client computer system" for computer systems 220a through 220i is intended in the context of maintaining presence information. In other words, the computer system 210 is a server computer system because it serves by maintaining presence information. The computer systems 220a through 220i are client computer systems because they are served by the server computer system 210 maintaining presence data. The use of the term "server computer system" for the server computer system 210 is not intended to imply that the server computer system 210 cannot also be a client computer system in a different context. Similarly, the use of the term "client computer system" for the client computer systems 220a through 220i is not intended to imply that the client computer systems cannot also be server computer systems in a different context.

In this description and in the following claims, "network connected" means having a connection either directly or indirectly through one or more networks. The solid line connecting each of client computer systems 220c through 220i to the server computer system 210 represents that these client computer systems are network connected to the server computer system 210. The dashed line connecting each of client computer systems 220a and 220b to the server computer system 210 represents that these client computer systems are not currently network connected to the server computer system 210 but are network connectable to the server computer system 210. In this description and in the

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

claims, "network connectable" means having the ability to connect either directly or indirectly through one or more networks.

The server computer system 210 maintains presence information regarding each of the plurality of client computer systems 220. In this description and in the claims, "presence information" concerning a given client computer system means information that describes the availability of a client computer system or a user of that client computer system. For example, "logged in" or "logged out" may describe whether the client computer system is network connected or not.

Figure 3 illustrates a data structure 300 that maintains presence data regarding each of the client computer systems 220a through 220i that are accessible by the server computer system 210. The data structure 300 includes a row entry 320a through 320i for each client computer system 220a through 220i. For each client computer system 220a though 220i, the data structure includes an identification field 310 that identifies the client computer system and a presence information field 315 that identifies presence information describing the availability of that client computer system.

For example, as described above, the client computer systems 220a and 220b are not network connected to the server computer system 210. Therefore, the data structure 300 indicates that client computer systems 220a and 220b are "logged out." Since the client computer system 220i is network connected to the server computer system 210, the data structure 300 indicates that client computer system 220i is "logged in." Since, as described above, the client computers 220c through 220h are network connected to the server computer system 210, the data structure 300 might indicate that those client computer systems are also "logged in." However, the data structure 300 indicates more

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

detailed presence information regarding the availability of those "logged in" client computer systems 220c through 220h.

For example, the data structure 300 indicates that the client computer systems 220c and 220d are "active" meaning that a user has used the computer so recently that the user is likely still at the computer. The data structure 300 also indicates that the client computer systems 220e and 220f are "idle" meaning that a user has not recently used the computer making it less likely that the user is at the computer. The presence information might also include information regarding the whereabouts of the user. For example, client computer system 220g is "at lunch" while the client computer system 220h is "out of the office until next Thursday."

The structure of Figures 1, 2 and 3 represents a system in which the present invention may operate. Although the server computer system 210 is network connectable to nine client computer systems in Figure 2, the server computer system 210 may be network connectable to more or less than nine client computer systems. Furthermore, the server computer system 210 may be connected to other server computer systems. In one example operating environment, the server computer system 210 is part of the constellation of computer systems that form the Internet.

Figure 4 illustrates a method 400 for controlling access to presence information in accordance with the present invention. The method of Figure 4 will be described with frequent reference to Figure 2 and occasional reference to Figure 3. In the example, the client computer system 220i of Figure 2 controls access to some of the presence information stored in the data structure 300 of Figure 3. In that sense, the client system 220i is the owner of that presence information. In the example described with reference to Figure 4, the client computer system 220i has the ability to control access to the presence

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

information that describes its own availability (the availability of the client computer system 220i).

In the method of Figure 4, acts performed exclusively by the owner client computer system such as the client computer system 220i are listed directly below the heading "CLIENT" on the left-hand side of Figure 4. Acts performed exclusively by the server computer system that maintains the presence information are listed directly below the heading "SERVER" on the right-hand side of Figure 4.

Referring to Figure 4, the owner client computer system creates a request that includes an instruction to set or change an access permission status (act 410) enforceable against at least a subset of the plurality of client computer systems 220 when those client computer system attempt to access the presence information of the owner client computer system. The request may set or change a variety of different access permission types. In this description and in the claims, the term "access permission type" means a way of limiting or granting access to presence information. For example, three types of access permission types which will be now be explained in further detail are entitled "presence", "subscriptions" and "send-to".

The "presence" access permission type may be used to control who can view accurate presence information. A participant who has "presence" access permission for the presence information associated with the owner client computer system 220i will thus be able to see that the owner client computer system 220i is "logged in". A participant who does not have such "presence" access permission will be unable to view accurate presence information regarding the owner client computer system 220i. A response to a request for such information from an unauthorized participant might include, for example, a deny message indicating that permission to view is denied, or may include inaccurate response

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

information. For example, the unauthorized participant may view that the owner client computer system 220i is "logged out" even though the system 220i is actually "logged in".

The "subscription" access permission type may be used to control who can view presence information, whether accurate or not. Figure 5 illustrates an extended data structure 500 for the owner client computer system 220i that will be used to describe the distinction and interrelation between the "presence" and "subscription" access permission types. The extended data structure 500 is shown only for the owner client computer system 220i although the other client computer systems 220a through 220h may have similar data structures. The extended portion of the data structure 500 includes access permission fields 510 that represent who is granted or denied what kind of access to the presence information.

For example, the access permission fields 510 indicate that client computer system 220a is denied "subscription" access permission to the presence information for the owner client computer system 220i. Also, the client computer system 220b is granted "subscription", but denied "presence" access permission. The client computer system 220c is granted "subscription" and "presence" access permission.

The client computer system 220a would be unable to view presence information regarding the owner client computer system 220i whether that presence information is real or manufactured since "subscription" access permission is denied. Also, the denied subscription permission would prevent the client computer system 220a from receiving notifications when the presence information for the owner client computer system 220i changes. Client computer systems 220b and 220c will be able to view some kind of presence information since they have "subscription" access permission. However, client computer system 220b is denied "presence" access permission thereby denying the right to

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

view accurate presence information. Thus, client computer system 220b will be able to view the manufactured presence information represented in the manufactured presence information field 520 of the extended data structure. In other words, client computer system 220b would perceive the owner client computer system 220i as being "logged out" when, in fact, the owner client computer system is "logged in". The client computer system 220c has "presence" access permission and thus would be able to view the accurate presence information indicating that the owner client computer system 220i is "logged out".

The "send-to" access permission type may be used to control who can send messages to the owner client computer system using the accessed presence information. For example, someone who does not have "sent-to" access permission status may be able to view the presence information of the owner client computer system, but will not be allowed to send messages using that presence information even though it indicates that the owner client computer system is "logged in" or "active". In particular, the "notify method" described in the WEBDAV GENA (General Notifications) protocol may be used to send the messages using accessed presence information.

Figure 6 illustrates a data structure 600 of a request to set or change the access permission status. The data structure includes one or more access control element fields 610a through 610n. Each access control element field may include a principle identifier field 612 that identifies the entity on which the access permission is to be enforced, a grant field 614 that identifies any access permission types granted to that entity, a deny field 616 that identifies any access permission types denied to that entity, and possibly an authentication field 618 that identifies the authentication types used to authenticate the

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

entity. Although these fields 612, 614, 616 and 618 are shown for the first access control element field 610, the other access control elements fields may each include similar fields.

The data structure 600 of the request may include an eXtensible Markup Language (XML) element that indicates the access permission type being denied or granted and to whom that access is denied or granted. Take the following XML element as an example.

```
<?xml version="1.0"?>
<a:rvpacl xmlns:a="http://schemas.microsoft.com/rvp/acl/">
    <a:acl>
        <a:inheritance>none</a:inheritance>
        <a:ace>
            <a:principal>
                <a:rvp-principal>
                    http://im.example.com/instmsg/aliases/220b/
                </a:rvp-principal>
                <a:credentials>
                    <a:assertion/>
                    <a:digest/>
                    <a:ntlm/>
                </a:credentials>
            </a:principal>
            <a:grant>
                <a:subscription/>
            </a:grant>
```

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

```
                    <a:deny>
                        <a:presence/>
                    </a:deny>
                </a:ace>
            </a:acl>
</a:rvpacl>
```

In this XML element, the portion between <a:ace> and </a:ace> defines an Access Control Element (ACE) that defines access permissions. This portion would correspond to the access control element field 610a shown in Figure 6. The portion of the access control element that occurs between <a:rvp-principal> and </a:rvp-principal> defines the entity to whom the access permission is to apply (corresponds to the principal identifier field 612 of Figure 6). In the above example request, the Uniform Resource Locator (URL) corresponding to the entity is "http://im.example.com/instmsg/aliases/220b/" which represents client computer system 220b. More specifically, the URL represents the user account on the presence information server (e.g., an instant messaging server) that the corresponding user using the client computer 220b is logged into. The portion of the access control element that occurs between <a:credentials> and </a:credentials> describes authentication mechanisms that may be used to authenticate the client computer system 220b when requesting access to presence information (corresponds to the authentication field 618 of Figure 6). The portion of the access control element between <a:grant> and </a:grant> describes the types of access permission granted (corresponds to the grant field 614 of Figure 6). In this example, client computer system 220b is granted "subscription" access permission. The portion of the access control element between <a:deny> and

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

</a:deny> describes the types of access permission denied (corresponds to the deny field 616 of Figure 6). In this example, client computer system 220b is denied "presence" access permission.

Once the owner client computer system generates the request to set or change access permission to the presence information (act 410), the owner client computer system then transmits the request to the server computer system (act 420). For example, the owner client computer system 220i may transmit to the server computer system 210 the request to grant "subscription" and deny "presence" access permission to the client computer system 220b.

Once the request is received at the server computer system (act 430), subsequent requests for accessing the present information will result in the server computer system determining whether or not to allow access to the presence information based on the request to set or change the access permission status. Accordingly, embodiments within the scope of the present invention include a means or step for determining whether or not to allow access to the presence information based on the request to set or change the access permission status.

In one embodiment, the server computer system sets the access permission fields 510 within the extended data structure 500 to represent the new access permissions (act 440). Then, upon receiving subsequent requests to access the presence information, the server computer system determines whether or not to grant the requested access based on the access permission fields 510 within the extended data structure 500 (act 450).

The above describes methods and systems for controlling access to presence information using a plurality of access permission types. Since many different access

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

permission types may be set, the present invention permits for fine grain control over what kind of access to the presence information is permitted.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed and desired to be secured by United States Letters Patent is:

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111